UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,404	11/03/2003	Benjamin Wilken	12221-020001	6346

26161 7590 03/26/2007

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,404	WILKEN ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-36 are rejected under 35 U.S.C. 102(e) as being anticipated by Malan(2002/0032871).

3. As per claim 1, Malan et al. discloses detecting scanning attacks[i.e. Dos attacks, 0028, 0057], adding host-pair connection records to a connection table each time a host accesses another host[0084]; at the end of a short update period, accessing the connection table to determine new host pairs; determining the number of new host pairs added to the table over the update period; and if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicating to a console that the new host is a scanner[0031, 0037, 0067, 0084].

4. As per claim 2, Malan discloses wherein "C1" and "C2" are adjustable thresholds[0084].

5. As per claim 3, Malan discloses wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table[0083-0084].

6. As per claim 4, Malan discloses aggregating records from the current time-slice table into a long update period table; and checking for ping scans at the end of a long update period; and

indicating hosts which produced more than "C3" new host pairs over the long update period[0029, 0032-0033, 0084].

7. As per claim 5, Malan discloses at the end of the long update period, accessing the long update connection table to determine new host pairs that the process had not determined before in the profile; determining the number of new host pairs added to the table over the long update period; and if a host has made more than a first threshold number "C4" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C5", then indicating the new host as a scanner[0083-0084].

8. As per claim 6, Malan discloses maintaining Address Resolution Protocol (ARP) packet statistics in the connection table and for sparse subnets tracking the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks[0081-0082].

9. As per claim 7, Malan discloses wherein the scanning attack is a ping scanning attack[0081].

10. As per claim 8, Malan discloses detecting port scanning attacks, the method includes retrieving from a connection table logged values of protocols and ports used for host pair connections in the table[0042-0043, 0045]; determining if the number of ports used in the historical profile is considerably smaller by a factor "C1" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly; and reporting a port scan to a console[0067-0068].

11. As per claim 9, Malan discloses assigning a severity level to the port scan and reporting the severity level of the port scan[0069].

12. As per claim 10, Malan discloses wherein the reported severity varies as a function of the deviation from historical norm[0068-0069].

13. As per claim 11, Malan discloses determining from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event[0081-0083].

14. As per claim 12, Malan discloses wherein determining occurs at the end of short update periods to detect normal scans[0084].

15. As per claim 13, Malan discloses wherein determining occurs at the end of long update periods to detect stealthy scans[0084].

16. As per claim 14, Malan discloses add host-pair connection records to a connection table each time a host accesses another host, at the end of a short update period, accessing the connection table to determine new host pairs; determine the number of new host pairs added to the table over the update period; and if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then indicate to a console that the new host is a scanner[0083-0084].

17. As per claims 15, 25, 29, Malan discloses wherein "C1" and "C2" are adjustable thresholds[0084].

18. As per claims 16, 26, 30, Malan discloses wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table[0037, 0083-0084].

19. As per claims 17, 27, 31, Malan discloses aggregate records from the current time-slice table into a long update period table; check for ping scans at the end of a long update period; and indicate hosts which produced more than "C3" new host pairs over the long update period[0029, 0032-0033, 0084].

20. As per claims 18, 32, Malan discloses access the long update connection table at the end of the long update period; determine the number of new host pairs added to the table over the long update period; and if a host has made more than a first threshold number "C4" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C5", then indicate the new host as a scanner[0067-0068, 0083-0084].

21. As per claim 19, Malan discloses maintain Address Resolution Protocol (ARP) packet statistics in the connection table; and track the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks[0081-0082].

22. As per claims 20, 33, Malan discloses causing a processor to: retrieve from a connection table logged values of protocols and ports used for host pair connections in the table[0042-0043, 0045]; determine if the number of ports used in the historical profile is considerably smaller by a factor "C1" than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold "C2", to record the anomaly; and report a port scan to a console[0067-0068].

23. As per claims 21, 34, Malan discloses assign a severity level to the port scan and report the severity level of the port scan[0069].

24. As per claims 22, 35, Malan discloses wherein the reported severity varies as a function of the deviation from historical norm[0068-0069].

25. As per claims 23, 36, Malan discloses determine from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event[0081-0083].

26. As per claims 24, 28, Malan discloses circuitry to add host-pair connection records to a connection table each time a host accesses another host, at the end of a short update period, accessing the connection table to determine new host pairs; circuitry to determine the number of new host pairs added to the table over the update period; and if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then circuitry to indicate to a console that the new host is a scanner[0067-0068, 0083-0084].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

March 21, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100